T0 - Práctica-(Trabajo de investigación) Ampliación de amenazas y análisis de ataques al Internet de las Cosas (IoT)

Alejandro Garcia Burguillos

19/09/2024

Introducción:

El Internet de las Cosas (IoT) se refiere a la interconexión de dispositivos físicos a través de Internet, permitiendo que estos dispositivos recopilen, compartan y analicen datos de manera autónoma. Desde cámaras de seguridad y electrodomésticos inteligentes hasta sensores industriales y automóviles conectados, el IoT está transformando la forma en que interactuamos con la tecnología y gestionamos nuestras vidas diarias.

Sin embargo, a medida que el número de dispositivos IoT sigue creciendo, también lo hacen los desafíos de seguridad asociados. Los casos de vulnerabilidades y ataques dirigidos a estos dispositivos han aumentado significativamente. Los ciberdelincuentes están explotando fallos de seguridad para acceder a datos sensibles, comprometer la privacidad de los usuarios y llevar a cabo ataques que pueden afectar tanto a individuos como a organizaciones. La creciente conectividad y la complejidad de estos dispositivos subrayan la necesidad urgente de mejorar las medidas de seguridad en el ámbito del IoT.

Noticia 1:
La nueva botnet de IoT "Raptor Train" compromete más de 200.000 dispositivos en todo el mundo

Raptor Train es una nueva botnet que ha emergido y se ha propagado rápidamente. Una botnet es una red de dispositivos comprometidos que los atacantes controlan remotamente para realizar actividades maliciosas.

La botnet ha afectado a más de 200,000 dispositivos IoT en todo el mundo.
Estos dispositivos incluyen cámaras de seguridad, routers, y otros aparatos conectados a Internet que suelen tener medidas de seguridad insuficientes.

Los atacantes detrás de Raptor Train utilizan varias técnicas para infectar dispositivos. Esto incluye explotar vulnerabilidades conocidas y utilizar credenciales predeterminadas o débiles. Una vez que un dispositivo está comprometido, se convierte en parte de la botnet y puede ser utilizado para realizar ataques DDoS o para enviar spam.

https://es.linkedin.com/pulse/la-nueva-botnet-de-iot-raptor-train-compromete-m%C3%A1s-200000-dispositivos-4iagc

Noticia 2:
Descubren una variante del gusano RapperBot, que infecta dispositivos IoT para lanzar ataques DDoS

RapperBot es una variante reciente de un gusano que se dirige a dispositivos IoT se infectan los dispositivos de la misma manera que la vista en la noticia anterior y su objetivo de uso es el mismo, igual que la anterior también aprovecha vulnerabilidades conocidas y contraseñas débiles para vulnerar el dispositivo y unirlo así a la red de bots mencionada.

https://www.europapress.es/portaltic/ciberseguridad/noticia-descubren-variante-gusano-rapperbot-infecta-dispositivos-iot-lanzar-ataques-ddos-20230418152548.html

Noticia 3:
Es posible robar un Tesla con un truco de radio barato con todo y su nueva tecnología sin llave

Usando un truco sencillo en el que se amplifica la señal de la llave se ha conseguido robar un coche de forma barata. Como dice la noticia aqui se demuestra que hay modelos de tesla que aun habiendo sido actualizados contra este problema sigue estando presente.

El método de los atacantes es sencillo, acercar el dispositivo de ampliación de señal hacia donde creen que está la llave, normalmente en la casa del dueño del coche, consiguiendo asi amplificarla y dirigirla hacia el coche para abrirlo con la propia señal de la llave.

https://es.wired.com/articulos/es-posible-robar-un-tesla-con-truco-de-radio-barato-con-todo-y-su-nueva-tecnologia-sin-llave

Noticia 4:
Conjunto de errores pone en acción a la empresa de software y a los fabricantes de dispositivos IoT

Investigadores de seguridad han encontrado múltiples vulnerabilidades en el software Kalay, desarrollado por la empresa taiwanesa Through Tek. Este software es utilizado en dispositivos de varias marcas para la transmisión de vídeo y otros datos a través de redes.

Las vulnerabilidades afectan a dispositivos de marcas como Roku, Wyze y Owlet. Los problemas de seguridad permiten a los atacantes potenciales acceder a datos sensibles, como transmisiones de video en vivo y otra información personal de los usuarios.

https://therecord.media/throughtek-kalay-software-vulnerabilities-roku-wyze-owlet